



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/696,629	10/29/2003	Michael R. Smith	CIS0195US	5549
33031 7590 12/09/2008 CAMPBELL STEPHENSON LLP 11401 CENTURY OAKS TERRACE BLDG. H, SUITE 250 AUSTIN, TX 78758				
EXAMINER NOBAHAR, ABDULHAKIM				
ART UNIT		PAPER NUMBER		
2432				
MAIL DATE		DELIVERY MODE		
12/09/2008		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/696,629

**Applicant(s)**

SMITH, MICHAEL R.

**Examiner**

ABDULHAKIM NOBAHAR

**Art Unit**

2432

**Period for Reply** -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 08 September 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-118 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-118 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/CDC)
- 4) ☐ Interview Summary (PTO-413)
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_
- Paper No(s)/Mail Date \_\_\_\_\_

#### **DETAILED ACTION**

1. This office action is in response to applicant's amendment filed on 09/08/2008.
2. Claims 1-118 are pending.
3. Claims 52, 71, 104 and 116 are amended.
4. Applicant's arguments regarding *§102 rejections* have been fully considered but they are not persuasive.
5. When responding to the Office action, Applicant is advised to clearly point out the patentable novelty the claims present in view of the state of the art disclosed by the reference(s) cited or the objection made. A showing of how the amendments avoid such references or objections must also be present. See 37 C.F.R. 1.111(c).

#### **Response to Arguments**

1. Applicants on page 26 of the remarks argue that the pertinence of the reference has not been clearly explained.

Examiner respectfully asserts that the cited portions of the reference are self-explanatory and are clear to a person of ordinary skill in the art at. Where ever any explanation was needed the examiner has added some descriptions to point out the pertinence of the cited portion of the reference to the recited limitations in the relevant claims.

2. Applicants on page 28 of the remarks argue that Williams fails to teach the limitations of the independent claims, as Williams is directed to the use of separate, individual security devices. The integrated approach and other features of the claimed

invention are simply not taught by Williams. For example, in the manner previously discussed, Williams is completely oblivious to the implementation of security labels, because Williams is not concerned with the integration of security in network devices, but merely stand-alone devices, among other distinctions.

Examiner respectfully disagrees and asserts that contrary to the applicant's submission, Williams discloses a system to provide network security. For example, Williams in the first paragraph of Summary in the specification describes:

"It is a further object of the invention to provide a secure network in which the security mechanisms are at layer 3 of protocol hierarchy. It is another object of the invention to provide a centralized administration of a layer 3 secure network that may be distributed over the Internet. It is another object of the invention to provide a security device that prevents unauthorized third parties from gaining access to a host. It is another object of the invention to provide a multi-level secure network having a security device coupled between each host and the network medium" which indicates that the Williams invention is for network security.

With regard to the "security labels", Williams discloses:

"In addition, since this is a Multi-Level Secure network, the NSC is responsible for defining the security levels and categories of information permitted on the network and the labeling used by each host". See forth paragraph of Summary.

"It ensures labeling of all data packets with a hierarchical security level and a set of non-hierarchical security categories appropriate for the local hosts". See col. 7, lines 2-4.

3. Examiner, however, in light of the above submission maintains the previous §102 rejection, objections of claims 18 and 94 and §101 rejection of claims 52-74 while considering the amendments to the claims and as follows.

### ***Claim Objections***

Claims 18 and 94 are objected to because of the following informalities: Claim 18 recites "third security level" and claim 94 recites "second security level". Examiner suggests that these claims should be amended to recite "a third security level" and "a second security level", respectively. Moreover, examiner suggests that for the purpose of clarity and consistency of claims, where ever in a claim a new element is introduced for the first time that element should be preceded with "a" or "an". For example, claims 1 and claim 33 should be amended to recite:

Claim 1: "comparing a first security level information and a second security level information".

Claim 33: "a computer readable medium...

a computer code, encoded..."

The same should be applied to other claims to become consistent with claims 52, 54, 55 and 56, for example.

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

**Claims 52-74** are rejected under 35 U.S.C. 101 because the claimed inventions are directed to non-statutory subject matter.

Although applicant has amended the claim 52, but this claim is still directed to a non-statutory subject matter, because it claims a computer program product that comprises a plurality of set of instructions, which form an assemblage of computer executable codes. The last limitation of claim 52 recites "computer readable storage media", which according to the paragraph [0085] of the specification on page 26 it could also be a carrier wave not a physical component. Even if the recited "computer readable storage media" considered to be a physical component, a computer program product cannot be comprised of a physical component. Thus, claim 52 is not statutory because the descriptions or expression of programs are not physical "things". They are neither computer components nor statutory processes, as they are not "acts" being performed. Therefore, claims 52-74 recite non-statutory subject matter.

### ***Claim Rejections - 35 USC § 102***

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

**Claims 1-118 are rejected under 35 U.S.C. 102(b) as being anticipated by Williams (US 6,304,973 B1).**

With regard to claims 1, 2, 11, 14, 27, 33, 34, 38, 39, 49, 52, 53, 57, 68, 71, 72, 76, 77, 87, 90, 94-96, 99, 101 and 109, Williams discloses:

A method and a system comprising:

- a network interface (see, e.g., abstract and 45-52);
- a processor (see, e.g., col. 19, lines 25-40);
- computer readable medium coupled to said processor (see, e.g., col. 19, lines 25-40);
- computer code, encoded in said computer readable medium (see, e.g., col. 19, lines 25-40),
- comparing first security level information and second security level information (see, e.g., col. 6, line 66-col. 7, line 4; col. 12, lines 42-67; col. 13, lines 22-30, where the security level of a host is the criteria to receive data; col. 14, lines 61-64), wherein said first security level information is stored in a security label of a packet received at a network node (see, e.g., col. 13, lines 38-54);
- said means for comparing is coupled to said network interface (see Figs. 1 through 3); and
- said second security level information is stored at said network node (see, e.g., col. 13, lines 22-43); and
- indicating processing to be performed on said packet based on said comparing (see, e.g., col. 13, lines 44-60, where the security device configured to permit packets labeled at multiple levels to pass corresponds to the recited indicating processing to be performed on the packet based on the result of comparing the security levels of the packet and the device);

wherein said means for indicating is coupled to said means for comparing (see Figs. 1 through 3 and Fig. 12; it is inherent that these two means are coupled to each other in a computer system to allow for verification of a packet; see also col. 14, lines 61-64 and col. 22, lines 33-41).

With regard to claims 3, 105 and 106, Williams discloses:

The method of claim 2, wherein

said first security level and said second security level implement one of a multi-level security paradigm (see, e.g., col. 13, lines 44-60) and a multi-lateral security paradigm (see, e.g., col. 5, lines 10-13; col. 6, lines 27-31, where multiple trusted VPNs provide trust among multiple hosts that corresponds to the recited multi-lateral security paradigm).

With regard to claim 4, an Official notice is taken of the following: the method of claim 2, wherein said security label is one of an enumerated security label and a bitmap security label.

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to utilize a security label in the types of an enumerated security label and a bitmap security label, because they are the types set by the "Standard Security Label for Information Transfer", FIPS PUB 188, of NIST published in September 1994.



With regard to claims 5, 91 and 98, Williams discloses:

The method of claim 2, wherein said second security level is a security level of a port of said network node (see, e.g., col. 3, lines 45-50; col. 5, lines 30-40).

With regard to claims 6 and 93, Williams discloses:

The method of claim 5, further comprising:

setting said security level of said port (see, e.g., col. 12, lines 52-55; col. 24, lines 19-25).

With regard to claims 7, 36, 40, 74, 78, 104, 107, 108, 110 and 111, Williams discloses:

The method of claim 6, wherein said setting said security level of said port comprises:

storing said second security level in a security label information field of an access control list entry (see, e.g., col. 1, lines 44-55; col. 5, lines 14-17; col. 6, line 66, where the security device has and enforces a security policy which implies that the security device has an access control list with entries).

With regard to claims 8, 37, 41, 56, 60, 75, 79, 112 and 114, Williams discloses:

The method of claim 6, wherein said setting said security level of said port comprises:

storing said second security level in a label range information field of a forwarding table entry (see, e.g., col. 14, lines 10-14 and 20-30).

With regard to claim 9, Williams discloses:

The method of claim 2, wherein said processing comprises:

dropping said packet, if said comparing indicates that said first security level is less than said second security level (see, e.g., col. 13, lines 55-63).

With regard to claim 10, Williams discloses:

The method of claim 2, wherein said processing comprises at least one of dropping said packet, redirecting said packet and rewriting said security label (see, e.g., col. 13, lines 55-63; col. 17, lines 28-36, where directing to a printer corresponds to the recited redirecting; col. 15, lines 13-16, where labeled at the correct level corresponds to the recited rewriting said security label).

With regard to claims 12 and 100, Williams discloses:

The method of claim 11, wherein

said security levels are a range of security levels (see, e.g., col. 13, lines 5-9).

With regard to claim 13, Williams discloses:

The method of claim 12, wherein said processing comprises:

dropping said packet, if said comparing indicates that said first security level is not within said range of security levels (see, e.g., col. 13, lines 10-21).

With regard to claims 15, 55 and 59, Williams discloses:

The method of claim 14, wherein said storing comprises:

storing said second security level in a security label information field of an access control list entry (see, e.g., col. 1, lines 44-55; col. 5, lines 14-17; col. 6, line 66, where the security device has and enforces a security policy which implies that the security device has an access control list with entries; col. 14, line 65).

With regard to claim 16, Williams discloses:

The method of claim 14, wherein said storing comprises:

storing said second security level in a label range information field of a forwarding table entry (see, e.g., col. 14, lines 10-14 and 20-30).

With regard to claims 17, 42, 61, 80 and 102, Williams discloses:

The method of claim 14, wherein said storing comprises:

communicating said second security level from a first network node by registering said second security level in a context (see, e.g., col. 11, lines 5-10; col. 13, lines 38-43; col. 14, line 1).

With regard to claims 18, 43, 62 and 81, Williams discloses:

The method of claim 17, wherein said registering comprises:

updating said second security level information by logically OR'ing third security level information with said second security level information (see, e.g., col. 12, lines 41-

50, where combination of the security levels corresponds to the recited OR'ing the security levels).

With regard to claims 19, 44, 63, 82 and 103, Williams discloses:

The method of claim 17, wherein

said context is a generic attribute registration protocol information propagation context (see, e.g., col. 4, lines 24-36; col. 18, lines 11-19), and

said registering said second security level is accomplished by said first network node issuing a join request (see, e.g., col. 15, lines 1-16).

With regard to claim 20, Williams discloses:

The method of claim 14, wherein said storing comprises:

storing said second security level in a label range information field of forwarding table (see, e.g., col. 14, lines 10-14 and 20-30).

With regard to claim 21, Williams discloses:

The method of claim 14, wherein said storing comprises:

storing said second security level in a port of said network node (see, e.g., col. 3, lines 45-50; col. 5, lines 30-40).

With regard to claims 22 and 92, Williams discloses:

The method of claim 21, wherein

said port is an egress port (see, e.g., Fig. 2, where the security device is an egress device located at the edge of the network).

With regard to claims 23, 45, 64 and 83, Williams discloses:

The method of claim 2, further comprising:

determining said first security level (see, e.g., col. 7, lines 1-4).

With regard to claims 24, 47, 66 and 85, Williams discloses:

The method of claim 23, wherein said determining comprises:

determining if an ingress port is marked as an access port (see, e.g., col. 7, lines 1-4); and

setting a security level of said ingress port to said first security level, if said ingress port is marked as an access port (see, e.g., col. 7, lines 13-20; col. 16, lines 26-33).

With regard to claims 25, 48, 67 and 86, Williams discloses:

The method of claim 24, further comprising:

setting said first security level information to said security level of said ingress port (see, e.g., col. 15, lines 10-16).

With regard to claims 26, 46, 65 and 84, Williams discloses:

The method of claim 23, further comprising:

authenticating a user having said first security level, wherein  
said determining is performed only if said user is authenticated (see, e.g., col. 3,  
lines 29-37; col. 4, lines 53-61; col. 7, lines 5-10).

With regard to claims 28, 50, 69 and 88, Williams discloses:

The method of claim 27, wherein said performing said processing  
comprises:

forwarding said packet, if said indicating indicates that said packet is allowed  
to be forwarded; and

dropping said packet, otherwise (see, e.g., col. 13, lines 10-21 and 55-63).

With regard to claim 29, Williams discloses:

The method of claim 27, wherein said performing said processing  
comprises:

forwarding said packet to a firewall, if said indicating indicates that said packet  
should be forwarded to said firewall (see, e.g., col. 7, lines 24-32).

With regard to claims 30, 51, 70, 89 and 97, Williams discloses:

The method of claim 2, further comprising:

stripping network security information from said packet; and adding subnetwork  
security information to said packet (see, e.g., col. 7, lines 1-5; col. 15, lines 13-16,

where labeling the packet to a correct level for transmission corresponds to the recited stripping... and adding security information).

With regard to claim 31, Williams discloses:

The method of claim 30, wherein

said network security information comprises said first security level information (see, e.g., col. 7, lines 13-22, where the passing of the packet through the security device to access a network implies that the security level of the network either is the same as the security level of the security device or at acceptable range and the security level of the packet is acceptable by security device).

With regard to claim 32, Williams discloses:

The method of claim 30, wherein

said subnetwork security information comprises said first security level information (see, e.g., col. 7, lines 13-22, where the passing of the packet through the security device to access a network implies that the security level of the network either is the same as the security level of the security device or at acceptable range and the security level of the packet is acceptable by security device).

With regard to claims 35, 54 and 73, Williams discloses:

The computer system of claim 34, wherein said computer code is further configured to cause said processor to:

set said security level of a port (see, e.g., col. 12, lines 52-55; col. 24, lines 19-25), wherein

said second security level is a security level of said port of said network node (see, e.g., col. 3, lines 45-50; col. 5, lines 30-40).

With regard to claim 113, Williams discloses:

The network device of claim 112, wherein said at least one forwarding table entry further comprises:

a port identifier field, wherein a port identifier stored in said port identifier field identifies a port (see, e.g., col. 6, lines 58-65; col. 15, lines 8-16 and line 66).

With regard to claim 115, Williams discloses:

The network device of claim 113, wherein said at least one forwarding table entry further comprises:

a media access control (MAC) address field (see, e.g., col. 5, lines 14-17; col. 6, lines 66-); and

a virtual local area network (VLAN) identifier field, wherein a combination of said MAC address field and said VLAN identifier field are associated with said port identifier field and said label range field (see, e.g., col. 5, lines 30-43; col. 11, lines 25-32; col. 26, lines 1-11).

With regard to claim 116, Williams discloses:



The network device of claim 113, wherein  
said media access control (MAC) address field is configured to store a MAC  
address (see, e.g., col. 5, lines 14-17; col. 6, lines 66-),  
said VLAN identifier field is configured to store a VLAN identifier ,  
said VLAN identifier identifies a VLAN, and  
a combination of said MAC address and said VLAN identifier identify said port  
and said security label (see, e.g., col. 5, lines 30-43; col. 11, lines 25-32; col. 26, lines 1-  
11).

With regard to claim 117, Williams discloses:

The network device of claim 114, wherein said at least one forwarding  
table entry further comprises:  
a media access control (MAC) address field configured to store a MAC  
address (see, e.g., col. 5, lines 14-17; col. 6, lines 66-), wherein  
said MAC address is associated with a security label stored in said  
label range field (see, e.g., col. 13, lines 1-9).

With regard to claim 118, Williams discloses:

The network device of claim 112, wherein said at least one forwarding table entry  
further comprises:  
a virtual local area network (VLAN) identifier field, wherein a VLAN identifier  
stored in said VLAN identifier field identifies a VLAN (see, e.g., col. 5, lines 30-43; col.  
11, lines 25-32; col. 26, lines 1-11), and

said VLAN is associated with a security label stored in said label range field (see, e.g., col. 13, lines 1-9).

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **ABDULHAKIM NOBAHAR** whose telephone number is (571)272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Abdulkhaleq Nobahar/  
Examiner, Art Unit 2132

December 3, 2008

/Gilberto Barron Jr/  
Supervisory Patent Examiner, Art Unit 2432